

Departamento de Engenharia Informática e de Sistemas  
Instituto Superior de Engenharia de Coimbra

**Licenciatura em Engenharia Informática**

**Segurança 2020/2021**



## **Configuração Avançada de um Equipamento**

Diogo Costa - 2018016581

Filipe Oliveira - 2018018618

Nuno Aparício - 2014014661

## Índice

Topologia .....	5
Introdução .....	6
Utilizadores.....	7
Telnet & SSH .....	7
Rotas .....	7
AAA e Logging .....	7
Configuração do Radius .....	7
Configuração do Syslog.....	9
Configurações básicas de segurança .....	9
Banners .....	9
Restrições nos inícios de sessão .....	10
Privilégios de administração.....	10
Utilizador Operador (oper) .....	11
Utilizador Administrador (adm).....	11
Utilizador Gestor (manager) .....	11
Configuração das Firewalls .....	11
Anti-spoofing a partir da internet.....	11
Anti-spoofing e RFC1918 para a internet .....	12
Time-Based .....	12
Reflexive.....	12
CBAC.....	13
Dynamic .....	14
Zone-based.....	15
Configuração do NAT .....	17
Conclusão.....	18

## Índice de Figuras

Figura 1 Topologia .....	5
Figura 2 WinRadius .....	8
Figura 3 Configuração AAA .....	8
Figura 4 Configuração Radius .....	8
Figura 5 Ambiente de Syslog .....	9
Figura 6 configuração syslog .....	9
Figura 7 Log de login .....	9
Figura 8 Banner MOTD e Login .....	10
Figura 9 Banner EXEC .....	10
Figura 10 Bloqueio de tentativas .....	10
Figura 11 Privilégios de Utilizador .....	10
Figura 12 Configuração de privilégios .....	10
Figura 13 Permissões do oper .....	11
Figura 14 Permissões adm .....	11
Figura 15 ACL Spoofing .....	11
Figura 16 Anti-Spoofing e RFC1918 .....	12
Figura 17 Aplicação de time-range a uma ACL .....	12
Figura 18 Configuração time-range .....	12
Figura 19 Configuração da ACL Reflected .....	13
Figura 20 ACL Reflected .....	13
Figura 21 syslog e radius ACL .....	13
Figura 22 Permissão ICMP com CBAC .....	13
Figura 23 Atribuição CBAC na Interface .....	13
Figura 24 Configuração Dynamic na ACL .....	14
Figura 25 Utilizador myaccess .....	14
Figura 26 ACL atribuída nas diferentes zonas .....	15
Figura 27 Criação de zonas .....	15
Figura 28 Atribuição das Zonas às Interfaces .....	15
Figura 29 Criação das Classes e atribuição das ACL's .....	15
Figura 30 Criação Policy-map e atribuição das classes .....	16
Figura 31 Criação da Zone-Pair .....	16
Figura 32 Atribuição de Outside e Inside nas Interfaces .....	17
Figura 33 ACL de IP's Privados .....	17
Figura 34 Configuração do NAT na Interface f0/0 .....	17

## Índice de Tabelas

Tabela 1 Endereços.....	6
Tabela 2 Utilizadores dos routers.....	7
Tabela 3 Utilizadores de VPCS .....	7

# Topologia

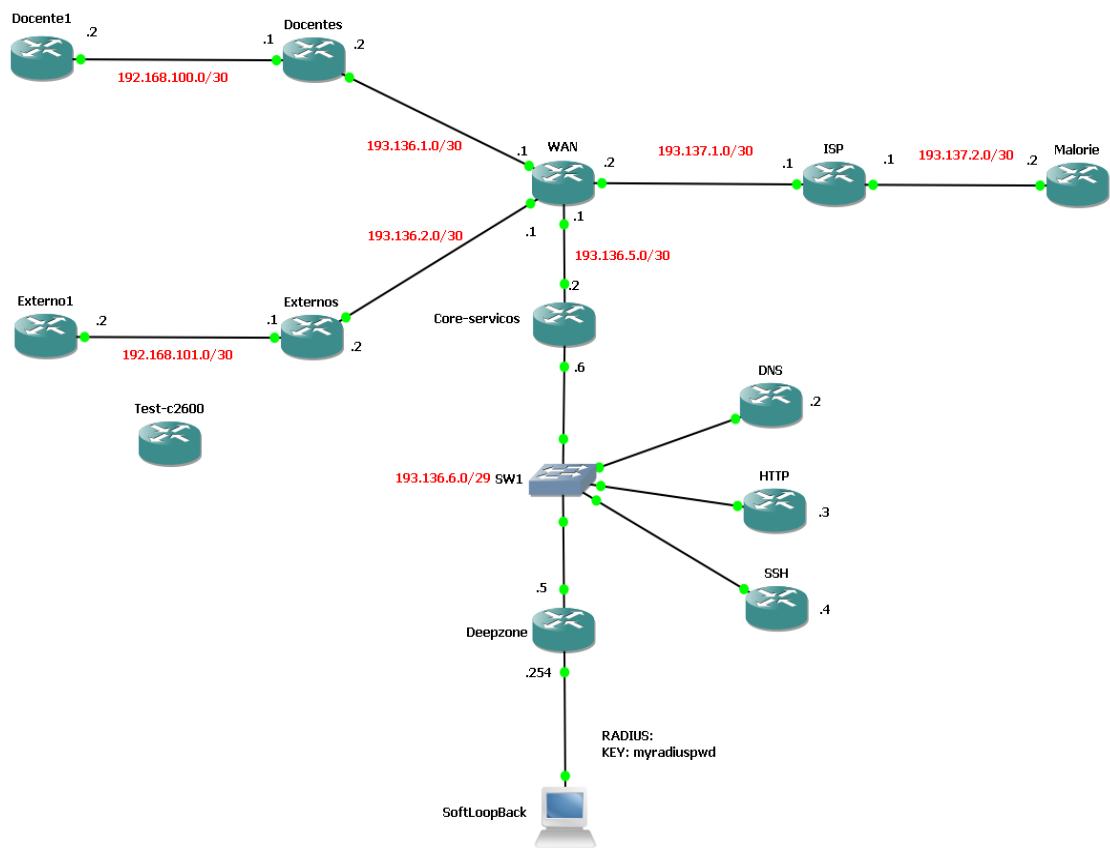


Figura 1 Topologia

## Introdução

Neste trabalho prático, o objetivo principal é conseguir estimular a aplicação prática dos conhecimentos adquiridos no âmbito das aulas de segurança, assim como promover a pesquisa de soluções técnicas que promovam as melhores práticas de segurança em redes.

Relativamente aos routers, foram apenas utilizados routers c7200 devido a ter problemas sendo todos os comandos do router *Externos* testados num router c2600 para verificar a sua compatibilidade. Seguem-se os IP's de cada router.

<b>Externo1</b>	f0/0: 192.168.101.2
<b>Externos</b>	f0/0: 193.136.2.2 f0/1: 192.168.101.1
<b>Docente1</b>	f0/0: 192.168.100.2
<b>Docentes</b>	f0/0: 193.136.1.2 f0/1 :192.168.101.1
<b>WAN</b>	e1/1: 193.136.2.1 e1/3:193.136.1.1 e1/0: 193.136.5.1 f0/0: 193.137.1.2
<b>ISP</b>	f0/0: 193.137.2.1 f0/1: 193.137.1.1
<b>Malorie</b>	f0/0: 193.137.2.2
<b>Core-Servicos</b>	f0/0: 193.136.5.2 f0/1: 193.136.6.6
<b>DNS</b>	f0/0: 193.136.6.2
<b>HTTP</b>	f0/0: 193.136.6.3
<b>SSH</b>	f0/0: 193.136.6.4
<b>DeepZone</b>	f0/0: 193.136.6.5 f0/1: 192.168.200.254
<b>SoftLoopback</b>	<b>192.168.200.2</b>

*Tabela 1 Endereços*

## Utilizadores

### Routers

Nome de Utilizador	Password
oper	operpwd
adm	admpwd
manager	manpwd

*Tabela 2 Utilizadores dos routers*

### Routers de VPCS

Nome de Utilizador	Password
oper	operpwd

*Tabela 3 Utilizadores de VPCS*

A password do Enable em todos os equipamentos é “myenapwd”.

## Telnet & SSH

Apenas dois routers possuem telnet nomeadamente o *Externos*, devido a este ser um router c2600 e não aceitar SSH, e o *WAN* pois foi necessário para a implementação da ACL Dynamic. Como o protocolo de aplicação telnet é pouco seguro decidimos aplicar nos restantes routers SSH e bloquear o telnet.

Ao reiniciar a topologia, a key de SSH não é guardada. Para que possa ser feito SSH aos equipamentos é necessário gerar a key nos equipamentos que o permitem com o seguinte comando:

**crypto key generate rsa general-keys modulus 1024**

## Rotas

O Router *WAN* tem rota default para sair para o router *ISP*.

*WAN* tem uma rota para a rede de *Docentes*, *Externos* e *Core-Servicos*.

*Core-Servicos* tem rotas para a *WAN*, rede abaixo (193.136.6.0/29) e rotas de saída para o *ISP*.

Relativamente ao Router *Deepzone* apenas tem rotas de saída.

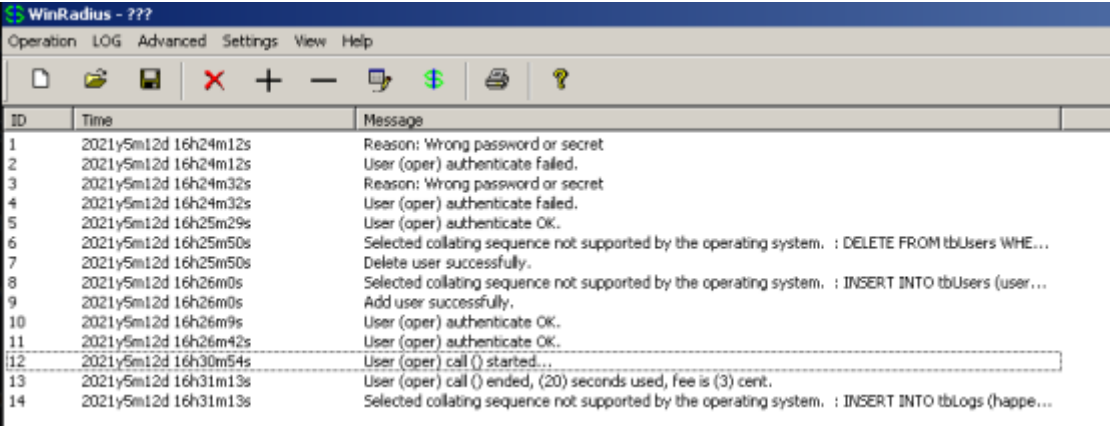
## AAA e Logging

### Configuração do Radius

Para esta configuração resolvemos usar o Radius que é um protocolo que opera nas portas 1812 e 1813, que fornece a autenticação centralizada, a autorização e a gestão contabilística (AAA) para os utilizadores que se ligam e utilizam o serviço de rede. A sua

principal função é autenticar utilizadores. Com a autenticação AAA, vai permitir que o Administrador da rede consiga configurar e acessar o dispositivo.

Usámos o Radius nos routers *Deepzone*, *Core-serviços*, *Wan*, *Externos* e *Docentes*. Sempre que exista uma autenticação realizada com sucesso ou falhada o Radius mostrará essa informação.



The screenshot shows the WinRadius application window with a menu bar (Operation, LOG, Advanced, Settings, View, Help) and a toolbar. Below is a table with three columns: ID, Time, and Message.

ID	Time	Message
1	2021y5m12d 16h24m12s	Reason: Wrong password or secret
2	2021y5m12d 16h24m12s	User (oper) authenticate failed.
3	2021y5m12d 16h24m32s	Reason: Wrong password or secret
4	2021y5m12d 16h24m32s	User (oper) authenticate failed.
5	2021y5m12d 16h25m29s	User (oper) authenticate OK.
6	2021y5m12d 16h25m50s	Selected collating sequence not supported by the operating system. : DELETE FROM tbUsers WHE...
7	2021y5m12d 16h25m50s	Delete user successfully.
8	2021y5m12d 16h26m0s	Selected collating sequence not supported by the operating system. : INSERT INTO tbUsers (user...
9	2021y5m12d 16h26m0s	Add user successfully.
10	2021y5m12d 16h26m9s	User (oper) authenticate OK.
11	2021y5m12d 16h26m42s	User (oper) authenticate OK.
12	2021y5m12d 16h30m54s	User (oper) call () started...
13	2021y5m12d 16h31m13s	User (oper) call () ended, (20) seconds used, fee is (3) cent.
14	2021y5m12d 16h31m13s	Selected collating sequence not supported by the operating system. : INSERT INTO tbLogs (happe...

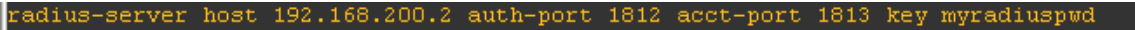
Figura 2 WinRadius



```
Deepzone(config)#do show run | i aaa
aaa new-model
aaa authentication login default local group radius
aaa authorization exec default local
aaa accounting exec default start-stop group radius
aaa session-id common
Deepzone(config)#
```

Figura 3 Configuração AAA

A key utilizada para o servidor radius é “myradiuspwd”.



```
radius-server host 192.168.200.2 auth-port 1812 acct-port 1813 key myradiuspwd
```

Figura 4 Configuração Radius



## Configuração do Syslog

O Servidor de Syslog foi configurado no IP 192.168.200.2.

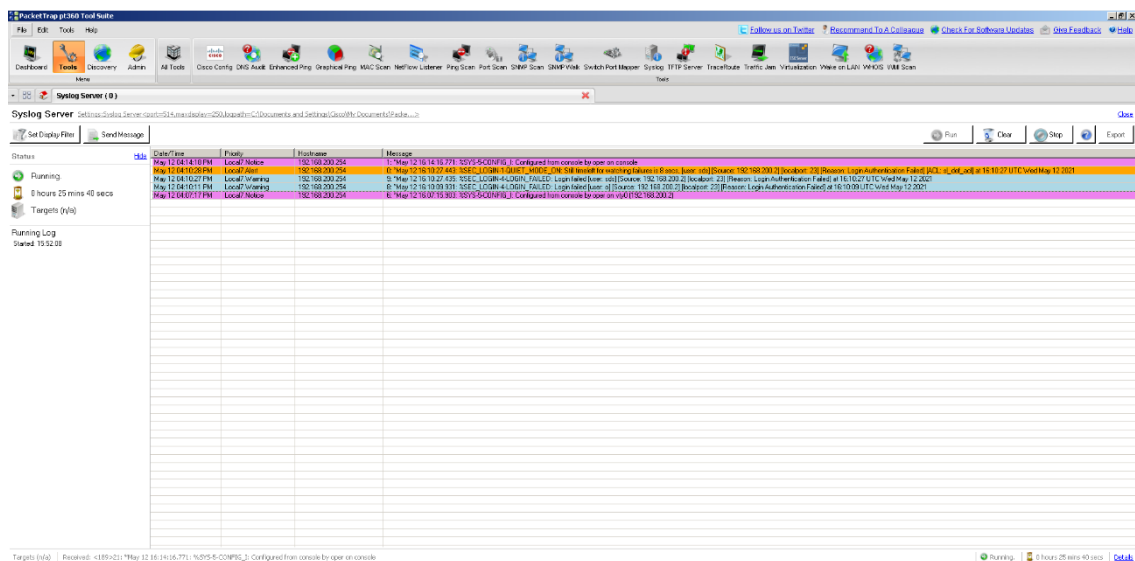


Figura 5 Ambiente de Syslog

A configuração do Syslog foi realizada nos routers *Deepzone*, *Core-serviços*, *WAN*, *Externos* e *Docentes*. Foi ativado o log de sucesso e insucesso do login.

```
logging trap notifications
logging 192.168.200.2
```

Figura 6 configuração syslog

```
login on-failure log
login on-success log
```

Figura 7 Log de login

## Configurações básicas de segurança

### Banners

Sempre que for iniciado um router aparecerão dois banners no qual serão indicadas algumas informações básicas.



No router *Externos* não foram realizadas as restrições pois o router c2600 não suporta vistas.

### Utilizador Operador (oper)

Este utilizador apenas pode aceder à interface de dentro e alterar a sua descrição. Devido a apenas ter essas permissões, deixámos a possibilidade de ser realizado um “show running-config”.

```
parser view permit-descritivo
secret 5 $1$hHmt$WFhdKB44ov6uqOxzHGfH3o
commands interface include description
commands configure include interface
commands exec include configure terminal
commands exec include configure
commands exec include show running-config
commands exec include show
commands configure include interface FastEthernet0/1
```

*Figura 13 Permissões do oper*

### Utilizador Administrador (adm)

Este utilizador pode fazer as alterações que quiser nas interfaces sendo que apenas não pode ligar ou desligar as mesmas. O mesmo, pode também verificar as informações acerca das interfaces.

```
parser view deny-shutdown
secret 5 $1$Qo4g$P.xfoxoFmBMU/pOxV9wvO.
commands interface exclude shutdown
commands configure include all interface
commands exec include configure terminal
commands exec include configure
commands exec include all show interfaces
commands exec include show
```

*Figura 14 Permissões adm*

### Utilizador Gestor (manager)

Este utilizador como tem controlo total sobre o equipamento, foi apenas definido que tem o nível de privilégio 15.

## Configuração das Firewalls

### Anti-spoofing a partir da internet

Para impedir o spoofing vindo do exterior bloqueámos todos os dados vindos da rede Malorie (Restrição 30).

```
Extended IP access list f0/0-in
10 permit tcp host 193.137.2.2 host 193.137.1.2 eq telnet
20 Dynamic users permit icmp host 193.137.2.2 host 193.136.6.2
30 deny ip 193.137.2.0 0.0.0.255 any
40 permit ip any any
```

*Figura 15 ACL Spoofing*

### Anti-spoofing e RFC1918 para a internet

Para resolver este problema criamos uma ACL standard em que negamos a passagem de dados de IPs Privados (RFC1918).

```
Standard IP access list f0/0-out
 10 deny 192.168.0.0, wildcard bits 0.0.255.255
 20 deny 10.0.0.0, wildcard bits 0.255.255.255
 30 deny 172.16.0.0, wildcard bits 0.15.255.255
 40 deny 224.0.0.0, wildcard bits 31.255.255.255
 50 deny 127.0.0.0, wildcard bits 0.255.255.255
 60 permit any
```

Figura 16 Anti-Spoofing e RFC1918

### Time-Based

Aplicámos a ACL Time-Based, para definir o período em que os utilizadores tenham a permissão de aceder à internet. Não sendo permitido qualquer ligação do exterior para estas redes.

O comando para configurar a ACL, baseada no tempo, é o time-range. Usado para especificar o período de tempo em que a declaração ACL é válida.

```
Extended IP access list f0/0-out
 5 deny ip 193.136.1.0 0.0.0.3 host 193.137.1.1 time-range FIM-SEMANA (inactive)
```

Figura 17 Aplicação de time-range a uma ACL

Ao executar este comando, é colocado no modo de configuração da lista de acesso no qual especificamos um intervalo de tempo periódico em que é bloqueado o acesso das 0h00m às 23h59m ao fim de semana.

```
time-range FIM-SEMANA
 periodic weekend 0:00 to 23:59
!
```

Figura 18 Configuração time-range

A declaração da lista de acesso só será processada quando a hora do router se enquadrar dentro do período especificado.

### Reflexive

Ao utilizar a access-list reflexive, o router acompanhará as ligações de saída e permitirá automaticamente o tráfego de retorno.

Para começar criámos uma access-list que vai permitir o telnet apenas através do soft-loopback.

```
Extended IP access list f0/0-in
10 permit icmp any any
40 deny ip 193.136.0.0 0.0.255.255 any
50 permit tcp host 192.168.200.2 any eq telnet reflect reflexive-acl (15 matches)
60 deny ip any any (10 matches)
```

Figura 19 Configuração da ACL Reflected

Depois de realizarmos um telnet à lista de acesso, esta irá criar a seguinte lista de acesso.

```
Reflexive IP access list reflexive-acl
 permit tcp host 193.136.2.2 eq telnet host 192.168.200.2 eq 2824 (15 matches) (time left 296)
```

Figura 20 ACL Reflected

Para permitir o tráfego de Radius & Syslog demos permissão apenas às portas de UDP 1812, 1813 e 514.

```
80 permit udp 193.136.0.0 0.0.255.255 host 192.168.200.2 eq syslog
90 permit udp 193.136.0.0 0.0.255.255 host 192.168.200.2 eq 1812
100 permit udp 193.136.0.0 0.0.255.255 host 192.168.200.2 eq 1813
```

Figura 21 syslog e radius ACL

## CBAC

O CBAC é capaz de verificar até a camada 7 do modelo OSI (Aplicação) e pode criar regras dinâmicas para permitir o tráfego de retorno. É semelhante à lista de acesso reflexive, mas uma das principais diferenças é que a ACL reflexive apenas verifica até à camada 4 (Transporte).

Primeiramente definimos os pacotes que queremos dar Inspect e assim permitir o ICMP com o CBAC.

```
ip inspect name CBAC icmp
```

Figura 22 Permissão ICMP com CBAC

E por fim definimos a interface que queremos que o CBAC atue.

```
interface FastEthernet0/1
 ip address 192.168.100.1 255.255.255.255
 ip access-group f0/1-in in
 ip access-group f0/1-out out
 ip nat inside
 ip inspect CBAC out
 ip virtual-reassembly in
 duplex auto
 speed auto
```

Figura 23 Atribuição CBAC na Interface

O CBAC teve de ser usado na rede Docentes devido aos routers c2600 não o permitirem.

## Dynamic

Para permitir que o *Malorie* consiga pingar o servidor DNS foi criado uma access-list dynamic para que, ao fazer telnet e entrar com as credenciais do myaccess o mesmo irá perder conexão e ativar o ICMP do *Malorie* para o DNS. Esta ligação de ICMP dura apenas 2 minutos.

```
Extended IP access list f0/0-in
 10 permit tcp host 193.137.2.2 host 193.137.1.2 eq telnet
 20 Dynamic users permit icmp host 193.137.2.2 host 193.136.6.2
 30 deny ip 193.137.2.0 0.0.0.255 any
 40 permit ip any any
```

Figura 24 Configuração Dynamic na ACL

Foi criado o utilizador myaccess com o comando “autocommand” para que este ative a dynamic.

```
username myaccess secret 5 $1$ACVE$Q8tQ/Clgd/JbFj5GB/OY50
username myaccess autocommand access-enable host timeout 2
```

Figura 25 Utilizador myaccess

Por aconselhamento do professor a ZBF deve ser aplicada no router *core-serviços*. Por consequência a ZBF não é compatível com a extended na mesma interface e como tal decidimos criar a dynamic na WAN permitindo assim o ping para o DNS a partir do *Malorie*.

## Zone-based

Na firewall Zone-Based a ideia é não atribuir listas de acesso a interfaces, mas criar diferentes zonas. Nas interfaces serão atribuídas as diferentes zonas e as políticas de segurança serão atribuídas ao tráfego entre as mesmas.

Primeiramente foi criada uma access-list extended numerada que será aplicada nas zonas criadas.

```
Extended IP access list 101
 10 permit tcp any host 193.136.6.2 eq domain
 20 permit tcp any host 193.136.6.3 eq www
 30 permit tcp any host 193.136.6.4 eq 22
 40 permit udp 192.168.0.0 0.0.255.255 any
 50 permit tcp 192.168.0.0 0.0.255.255 any (6 matches)
 60 permit udp 193.136.0.0 0.0.255.255 any (1113 matches)
 70 permit icmp any any (2806 matches)
```

Figura 26 ACL atribuída nas diferentes zonas

De seguida foram criadas 2 zonas.

```
zone security FO/0
description externa
zone security FO/1
description zona dmz
```

Figura 27 Criação de zonas

O próximo passo foi atribuir as zonas às interfaces adequadas.

```
interface FastEthernet0/0
ip address 193.136.5.2 255.255.255.252
zone-member security FO/0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 193.136.6.6 255.255.255.248
zone-member security FO/1
duplex auto
speed auto
```

Figura 28 Atribuição das Zonas às Interfaces

De seguida criámos as classes e atribuímos as respectivas access-lists a cada uma das classes.

```
class-map type inspect match-all f0/0-class
match access-group 101
class-map type inspect match-all f0/1-class
match access-group 101
```

Figura 29 Criação das Classes e atribuição das ACL's

Depois criamos a policy-map e damos permissão para o “inspect” de cada uma das classes

```
policy-map type inspect f0/0-policy
  class type inspect f0/0-class
    inspect
  class class-default
    drop
policy-map type inspect f0/1-policy
  class type inspect f0/1-class
    inspect
  class class-default
    drop
```

*Figura 30 Criação Policy-map e atribuição das classes*

Por fim definimos a nossa “zone-pair” atribuindo as zonas de source e destination. Damos também permissão à policy criada anteriormente.

```
zone-pair security f0/0-f0/1 source F0/0 destination F0/1
  service-policy type inspect f0/0-policy
zone-pair security f0/1-f0/0 source F0/1 destination F0/0
  service-policy type inspect f0/1-policy
```

*Figura 31 Criação da Zone-Pair*



## Configuração do NAT

Ao configurar o NAT permitimos às redes privadas que utilizam endereços IP não registados se conectem à Internet. O NAT opera nos Routers *Externos* e *Docentes*, e traduz os endereços privados na rede interna em endereços legais, antes de os pacotes serem encaminhados para outra rede.

Por exemplo, a rede *Externos* (192.168.101.0/30) envia um pacote para a rede externa. Sem a configuração do NAT este pacote sairia com o IP privado. Ao aplicar o NAT no router *Externos* definimos que todos os pacotes que saiam da rede 192.168.101.0 saiam com o IP público. Este IP está presente na interface f0/0 do router *Externos*. O mesmo se aplica para a rede *Docentes*.

1º Define-se quais as interfaces de saída e de entrada.

```
interface FastEthernet0/0
ip address 193.136.1.2 255.255.255.252
ip access-group f0/0-in in
ip access-group f0/0-out out
ip nat outside
ip virtual-reassembly in
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 192.168.100.1 255.255.255.252
ip access-group f0/1-in in
ip access-group f0/1-out out
ip nat inside
ip inspect CBAC out
ip virtual-reassembly in
```

Figura 32 Atribuição de Outside e Inside nas Interfaces

2º Em seguida, configurámos uma ACL que inclui uma lista dos endereços de origem internos que serão traduzidos.

```
Standard IP access list 1
10 permit 192.168.100.0, wildcard bits 0.0.0.255
```

Figura 33 ACL de IP's Privados

3º Por fim, ativamos o NAT.

```
ip nat inside source list 1 interface FastEthernet0/0 overload
```

Figura 34 Configuração do NAT na Interface f0/0

## Conclusão

Baseado no que acabámos por realizar neste trabalho prático, uma pessoa com conhecimentos básicos de GNS3 e CISCO, conseguirá através deste relatório espelhar na sua imagem Windows XP exatamente os mesmos procedimentos que nós utilizámos e assim entender mais acerca de serviços de segurança com aplicação de firewalls, logging, autenticação, autorização bem como a configuração do NAT.